



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/998,915	11/30/2001	Francisco J. Villavicencio	21756-012200	4254

51206 7590 03/13/2006

TOWNSEND AND TOWNSEND AND CREW LLP
TWO EMBARCADERO CENTER
8TH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

JEAN GILLES, JUDE

ART UNIT	PAPER NUMBER
----------	--------------

2143

DATE MAILED: 03/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/998,915

Applicant(s)

VILLAVICENCIO, FRANCISCO J.

Examiner

Jude J. Jean-Gilles

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 December 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-48 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-48 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>03/14/2005</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This Action is in regards to the Reply received on 12/16/2005.

Response to Amendment

1. This action is responsive to the application filed on 12/16/2005. Prior to the entry of this Amendment, claims 1-48 were pending in this Application. Claims 1, 2, 5, 6, 8, 10-17, 19, 21-24, 28, 30-35, 37-39, 41-45, 47, and 48 are amended herein. No claims have been added and no claims have been canceled. Therefore claims 1-48 remain pending in this application. Examiner has respectfully reconsidered all of these claims as amended and requested by the Applicant requests for at least the reasons presented in the Reply of 12/16/2005. Claims 1-48 represent a method and apparatus for an "impersonation in an access system."

Response to Arguments

2. Applicant's arguments with respect to claims 1, 16, 24, 28, 35, 39, and 45 have been carefully considered, but are not deemed fully persuasive. Applicant's arguments are deemed moot in view of the following new ground of rejection as explained here below, necessitated by Applicant substantial amendment [i.e., a method of allowing a first user (instead of a first entity which was broadly interpreted in the First Office Action) to impersonate a second user for resource access] to the claims which significantly affected the scope thereof.

The dependent claims stand rejected as articulated in the First Office Action and all objections not addressed in Applicant's response are herein reiterated.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 1-48** are rejected under 35 U.S.C. 103(a) as being unpatentable over Boltz et al. (Boltz) US Patent No. 6,981,043 B2 in view of Purpura et al (Purpura) U.S. Patent No. 6,421,768 B1.

Regarding claim 1, Boltz discloses a method of allowing a first user to impersonate a second user (column 12, lines 1-14; column 17, lines 8-17), the method, comprising the steps of:

receiving authentication credentials for a first user and an identification of a second user (column 12, lines 1-14; column 17, lines 8-17);

authenticating said first user based on said authentication credentials for said first user (column 12, lines 1-14; column 17, lines 8-17); however, Boltz does not specifically disclose the details of "creating a cookie that stores an indication of said second user if said step of authenticating is performed successfully; and authorizing said first user to access a first resource as said second user based on said cookie (column 3, lines 27-48; column 3, lines 27-59).

In the same field of endeavor, Purpura discloses a (...once the first computer 110 authenticates the user, such authentication may be transferred to the second computer 120 as follows. The first computer 110 uses a data structure for passing the authentication to the second computer 120. In an exemplary embodiment particularly well suited for Internet applications, the data structure could be a cryptographically assured cookie 150 that is made by creating a cryptographically assured voucher 160 at the first computer 110, and embedding the voucher 160 into the cookie 150 for transmission to the user's computer 100 and hence to the second computer 120....) [see *Purpura*, column 3, lines 27-48].

Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Purpura's teachings of a method and apparatus for creating a cookie that stores a user- indication for authorization access with the teachings of Boltz for the purpose correlating different user identities in different environments that describe the same user to reduce costs as stated by Boltz in lines 1-8 of column 2. By this rationale **claim 1** is rejected.

Regarding claim 2, The combination of Boltz-Purpura discloses a method according to claim 1, further comprising the step of: providing a form for said authentication credentials, said form includes a request for a user identification, a password and an impersonated identification, said user identification and said password correspond to said authentication credentials for said first user, said impersonated

identification corresponds to said identification of said second user (see Purpura; column 3, lines 37-59; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 3, The combination of Boltz-Purpura discloses a method according to claim 1, wherein: said step of receiving is performed by an access system; said access system protects said first resource; and said first resource is separate from said access system (see Purpura; column 3, lines 27-69).

Regarding claim 4, The combination of Boltz-Purpura discloses a method according to claim 1, wherein: said step of receiving is performed by an access system; said access system protects a plurality of resources; and said plurality of resources includes said first resource (see Purpura; column 3, lines 27-69).

Regarding claim 5, The combination of Boltz-Purpura discloses a method according to claim 1, wherein: said cookie stores a distinguished name of said second user and an IP address for said first user (see Purpura; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 6, The combination of Boltz-Purpura discloses a method accord to claim 1, further comprising the steps of:

receiving a request to access said first resource; providing a form for said authentication credentials, said form includes a request for a user identification, a password and an impersonates identification, said user identification and said password correspond to said authentication credentials for said first user, said impersonated identification corresponds to said identification of said second user; and transmitting

Art Unit: 2143

said cookie for storage on a device being used by said first user to send said request to access said first resource (see Purpura; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 7, The combination of Boltz-Purpura discloses a method according to claim 1, wherein: said steps of receiving, authenticating and authorizing are performed by an access system; said access system provides access management services and identity management services; and said first resource is protected by, but separate from, said access system (see Purpura; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 8, The combination of Boltz-Purpura discloses a method according to claim 1, wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile (see Purpura; column 3, lines 27-67),

searching said directory server for a second user identity profile that matches said identification of said second user(see Purpura; column 3, lines 27-67; see Boltz; column 3, lines 27-48; column 3, lines 27-59), and

accessing one or more attributes of said second user identity profile ; see Boltz; column 3, lines 27-48; column 3, lines 27-59; and

said cookie includes said one or more attributes of said second user identity profile (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 9, The combination of Boltz-Purpura discloses a method according to claim 8, wherein: said steps of searching a directory server for a first user identity profile and verifying said password based on said user identity profile are performed by a first authentication plug-in (see Purpura; column 3, lines 27-67); and said steps of searching said directory server for a second user identity profile and accessing one or more attributes of said second user identity profile are performed by a second authentication plug-in (see Purpura; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 10, The combination of Boltz-Purpura discloses a method according to claim 1, wherein: said cookie stores a distinguished name for said second user; and said step of authorizing includes the steps of: accessing said distinguished name stored in said cookie, accessing a user identity profile for said second user based on said distinguished name, accessing a set of one or more authorization rules for said first resource, and comparing attributes of said user identity profile for said second user to said set of one or more authorization rules for said first resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 11, The combination of Boltz-Purpura discloses a method according to claim 1, wherein: said authentication credentials correspond to a set of attributes for said first user; said identification of said second user corresponds to a set of attributes for said second user; said step of authorizing is based on one or more of said attributes for said first user; and said step of authorizing is based on one or more of

said attributes for said second user (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 12, The combination of Boltz-Purpura discloses a method according to claim 1, wherein: said authentication credentials correspond to a set of attributes for said first user; and said step of authorizing is not based on attributes for said first user (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 13, The combination of Boltz-Purpura discloses a method according to claim 1, further comprising the steps of: receiving a request for a login form; and providing said login form, said login form includes a request for a user identification, a password and an impersonated identification, said user identification and said password correspond to said authentication credentials for said first user, said impersonated identification corresponds to said identification of said second user. includes said first resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 14, The combination of Boltz-Purpura discloses a method according to claim 1, further comprising the steps of: receiving a request from said first user to access a second resource after said step of creating said cookie; accessing contents of said cookie and determining not to authenticate said first user in response to said request to access said second resource; and authorizing said first user to access said second resource as said second user based on said cookie, said step of authorizing said first user to access said second resource is performed without

Art Unit: 2143

authenticating said first user in response to said request to access said second resource. includes said first resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 15, The combination of Boltz-Purpura discloses a method according to claim 1, wherein: said steps of authenticating and authorizing are performed without knowing a password for said second user includes said first resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 16, The combination of Boltz-Purpura discloses a method for impersonating, comprising the steps of:

receiving authentication credentials for an impersonator and an identification of a impersonatee at an access system, said access system protects a first resource that is separate from said access system column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15);

authenticating said first impersonator based on said authentication credentials for said impersonator, wherein said step of authenticating is performed by said access system (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15); and

authorizing said impersonator to access said first resource as said impersonatee, said step of authorizing is performed by said access system includes said first resource (; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Art Unit: 2143

Regarding claim 17, The combination of Boltz-Purpura discloses a method according to claim 16, wherein:

said steps of authenticating and authorizing are performed without knowing a password for said impersonatee (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 18, The combination of Boltz-Purpura discloses a method according to claim 16, wherein:

said access system protects a plurality of resources that are separate from said access system; and said plurality of resources includes said first resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 19, The combination of Boltz-Purpura discloses a method according to claim 16, wherein:

said authentication credentials include an ID and a password (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15);

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,

verifying said password based on said user identity profile (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15),

searching said directory server for a second user identity profile that matches said identification of said impersonate (see Purpura; column 3, lines 27-67;

Art Unit: 2143

column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59), and

accessing one or more attributes of said second user identity profile; and said step of authorizing uses said one or more attributes of said second user identity profile (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 20, The combination of Boltz-Purpura discloses a method according to claim 16, wherein:

said steps of searching a directory server for a first user identity profile and verifying said password based on said user identity profile are performed by a first authentication plug-in (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15); and

said steps of searching said directory server for a second user identity profile and accessing one or more attributes of said second user identity profile are performed by a second authentication plug-in (see Purpura; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 21, The combination of Boltz-Purpura discloses a method according to claim 16, wherein:

said step of authenticating provides a name for said impersonate (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15), and

said step of authorizing includes the steps of: accessing said name,

accessing a user identity profile for said impersonate based on said name, accessing a set of one or more authorization rules for said resource, and comparing attributes of said user identity profile for said impersonate to said set of one or more authorization rules for said resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 22, The combination of Boltz-Purpura discloses a method according to claim 16, wherein:

said authentication credentials correspond to a set of attributes for said impersonator; said identification of said impersonate corresponds to a set of attributes for said impersonatee; wherein said step of authorizing is based on one or more of said attributes for said impersonator; and said step of authorizing is based on one or more of said attributes for said impersonatee (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 23, The combination of Boltz-Purpura discloses a method according to claim 16, further comprising the steps of:

receiving a request to access a second resource from said impersonator after said step of authenticating said impersonator, said access system protects said second resource; and authorizing said impersonator to access said second resource as said impersonatee, said step of authorizing said impersonator to access said second resource is performed without authenticating said impersonator in response to said

Art Unit: 2143

request to access said second resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 24, The combination of Boltz-Purpura discloses a method for impersonating, comprising the steps of:

receiving authentication credentials for the first entity and an identification of a second entity at an access system, wherein said access system protects a plurality of resources; receiving an indication of one or more of said plurality of resources(see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15);

authenticating said first entity based on said authentication credentials for said first entity, said step of authenticating is performed by said access system (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15); and

authorizing said first entity to access said one or more of said plurality of resources as said second entity, wherein said step of authorizing is performed by said access system(see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 25, The combination of Boltz-Purpura discloses a method according to claim 24, wherein:

said authentication credentials include an ID and a password (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15);

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15)'

verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said second entity, and accessing one or more attributes of said second user identity profile; and said step of authorizing uses said one or more attributes of said second user identity profile (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 26, The combination of Boltz-Purpura discloses a method according to claim 24, wherein: said step of authenticating provides a name for said second entity; and said step of authorizing includes the steps of: accessing said name, accessing a user identity profile for said second entity based on said name, accessing a set of one or more authorization rules for said resource, and comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 27, The combination of Boltz-Purpura discloses a method according to claim 24, wherein: said authentication credentials correspond to a set of attributes for said first entity; said identification of said second entity corresponds to a set of attributes for said second entity; said step of authorizing is based on one or more attributes for said first entity; and said step of authorizing is not based on attributes for

Art Unit: 2143

said first entity (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 28, The combination of Boltz-Purpura discloses one or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving authentication credentials for a first user and an identification of a second user (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15); authenticating said first user based on said authentication credentials for said first user; creating a cookie that stores an indication of said second user if said step of authenticating is performed successfully (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59); and

authorizing said first user to access a first resource as said second user based on said cookie (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 29, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 28, wherein: said steps of receiving, authenticating and authorizing are performed by an access system; said access system protects a plurality of resources separate from said access system; and said plurality of resources includes said first resource (see Purpura; column 3, lines 27-

Art Unit: 2143

67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 30, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 28, wherein: said cookie stores a distinguished name of said second user and an IP address for said first user (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 31, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 28, wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of: searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said second user, and accessing one or more attributes of said second user identity profile; and said cookie includes said one or more attributes of said second user identity profile (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 32, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 28, wherein: said cookie stores a distinguished name for said second user; and said step of authorizing includes the steps of: accessing said distinguished name stored in said cookie, accessing a user identity profile for said second user based on said distinguished name, accessing a set of one or more authorization rules for said first resource, and comparing attributes of said user identity profile for said second user to said set of one or more authorization

Art Unit: 2143

rules for said first resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 33, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 28, wherein: said authentication credentials correspond to a set of attributes for said first user; said identification of said second user corresponds to a set of attributes for said second user; said step of authorizing is based on one or more of said attributes for said first user; and said step of authorizing is based on one or more of said attributes for said second user (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 34, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 28, wherein: receiving a request from said first user to access a second resource after said step of creating said cookie; accessing contents of said cookie and determining not to authenticate said first user in response to said request to access said second resource; and authorizing said first user to access said second resource as said second user based on said cookie, said step of authorizing said first user to access said second resource is performed without authenticating said first user in response to said request to access said second resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 35, The combination of Boltz-Purpura discloses an apparatus for providing access management that allows for impersonating, comprising:

a communication interface (see Purpura; column 5, lines 16-33);
a storage device (fig. 1, items 100, 110, and 120); and
a processing unit in communication with said communication interface and said storage device, said processing unit performs a method comprising the steps of:

receiving authentication credentials for a first user and an identification of a second user (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59),

authenticating said first user based on said authentication credentials for said first user (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15),

creating a cookie that stores an indication of said second user if said step of authenticating is performed successfully, and authorizing said first user to access a first resource as said second user based on said cookie (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 36, The combination of Boltz-Purpura discloses an apparatus according to claim 35, wherein: said steps of receiving, authenticating and authorizing are performed by an access system; said access system protects a plurality of resources separate from said access system; and said plurality of resources includes said first resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 37, The combination of Boltz-Purpura discloses an apparatus according to claim 35, wherein: said authentication credentials include an ID and a

Art Unit: 2143

password; said step of authenticating includes the steps of: searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said second user, and accessing one or more attributes of said second user identity profile; and said cookie includes said one or more attributes of said second user identity profile (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 38, The combination of Boltz-Purpura discloses an apparatus according to claim 35, wherein: said cookie stores a distinguished name for said second user; and said step of authorizing includes the steps of: accessing said distinguished name stored in said cookie, accessing a user identity profile for said second user based on said distinguished name, accessing a set of one or more authorization rules for said first resource, and comparing attributes of said user identity profile for said second user to said set of one or more authorization rules for said first resource (see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 39, The combination of Boltz-Purpura discloses one or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving authentication credentials for a impersonator and an identification of a impersonatee at an access system, said access system protects a first resource that is

Art Unit: 2143

separate from said access system (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

authenticating said impersonator based on said authentication credentials for said impersonator, said step of authenticating is performed by said access system (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15); and

authorizing said impersonator to access said first resource as said impersonatee, said step of authorizing is performed by said access system (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 40, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 39, wherein: said access system protects a plurality of resources that are separate from said access system; and said plurality of resources includes said first resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 41, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 39, wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of: searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said impersonatee, and accessing one or more attributes of said second user identity profile; and said step of authorizing uses said one or more attributes of said second user

identity profile (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-67; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 42, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 39, wherein: said step of authenticating provides a name for said impersonator; and said step of authorizing includes the steps of: accessing said name, accessing a user identity profile for said impersonatee based on said name, accessing a set of one or more authorization rules for said resource, and comparing attributes of said user identity profile for said impersonatee to said set of one or more authorization rules for said resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-67; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 43, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 39, wherein: said authentication credentials correspond to a set of attributes for said impersonator; said identification of said impersonatee corresponds to a set of attributes for said impersonatee; said step of authorizing is based on one or more of said attributes for said impersonator; and said step of authorizing is based on one or more of said attributes for said impersonatee (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-67; see Boltz; column 3, lines 27-48, column 3, lines 27-59).

Regarding claim 44, The combination of Boltz-Purpura discloses one or more processor readable storage devices according to claim 39, wherein said method further comprises the steps of: receiving a request to access a second resource from said

Art Unit: 2143

impersonator after said step of authenticating said impersonator, said access system protects said second resource; and authorizing said impersonator to access said second resource as said impersonatee, said step of authorizing said impersonator to access said second resource is performed without authenticating said impersonator in response to said request to access said second resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-67; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 45, The combination of Boltz-Purpura discloses an apparatus for providing access management that allows for impersonating, comprising:

a communication interface (see Purpura; column 5, lines 16-33);

a storage device (fig. 1, items 100, 110, and 120); and

a processing unit in communication with said communication interface and said storage device, said processing unit performs a method comprising the steps of:

receiving authentication credentials for a impersonator and an identification of a impersonatee at an access system, said access system protects a first resource that is separate from said access system (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59),

authenticating said impersonator based on said authentication credentials for said impersonator, said step of authenticating is performed by said access system (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15), and

authorizing said impersonator to access said first resource as said

impersonatee, said step of authorizing is performed by said access system (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 46, The combination of Boltz-Purpura discloses an apparatus according to claim 45, wherein: said access system protects a plurality of resources that are separate from said access system; and said plurality of resources includes said first resource(see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 47, The combination of Boltz-Purpura discloses an apparatus according to claim 45, wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of: searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said impersonatee, and accessing one or more attributes of said second user identity profile; and said step of authorizing uses said one or more attributes of said second user identity profile (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-67; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Regarding claim 48, The combination of Boltz-Purpura discloses an apparatus according to claim 45, wherein: said step of authenticating provides a name for said impersonatee; and said step of authorizing includes the steps of: accessing said name, accessing a user identity profile for said impersonatee based on said name, accessing a set of one or more authorization rules for said resource, and comparing attributes of

said user identity profile for said impersonatee to said set of one or more authorization rules for said resource (see Purpura; column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-67; see Boltz; column 3, lines 27-48; column 3, lines 27-59).

Response to Arguments

5. Applicant's Request for Reconsideration filed on 12/16/2005 has been carefully considered but is not deemed fully persuasive. However, because there exists the likelihood of future presentation of this argument, the Examiner thinks that it is prudent to address Applicants' main points of contention.

Applicant contends that Purpura discloses a single sign-on method that, as is typical, of single sign-on, allows a user to access a second computer system based on his access of a first computer system. In other words, under Pupura, a user can logon to or access a first system which performs any necessary authentication. The first system then issues a token, in this case, a "cryptographically assured cookie" to the user. The same user can then use this token to access other systems without re-authenticating. However, Purpura does not disclose impersonation, i.e., authorizing a first user to access a system or resource as a second user. The Claimed invention should be allowed based on this characterization of the prior art.

It is the position of the Examiner that Purpura teaches the limitations of the above mentioned claims, but not in specific details. However, in view of Applicant's remarks, new patent of Boltz is used to address this characterization of the invention. Boltz

Art Unit: 2143

discloses "once the user is authenticated for one environment, the identity mapping mechanism of the preferred embodiments can be used to find an appropriate identity in a different user registry that is associated with the authenticated user, and impersonate the associated identity or otherwise apply the security semantics of the second user registry in order to access data protected by its security semantics. " [see Boltz; column 3, lines 27-48, column 3, lines 27-59]. Claims 1-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boltz et al. (Boltz) US Patent No. 6,981,043 B2 in view of Purpura et al (Purpura) U.S. Patent No. 6,421,768 B1. In light of the above prima facie obviousness case, the rejection is sustained.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2143

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7. Any inquiry concerning this communication or earlier communications from examiner should be directed to Jude Jean-Gilles whose telephone number is (571) 272-3914. The examiner can normally be reached on Monday-Thursday and every other Friday from 8:00 AM to 5:30 PM.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley, can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-9000.


Jude Jean-Gilles

Patent Examiner

Art Unit 2143

JJG 

March 03, 2006


DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100